(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 June 2002 (20.06.2002)

PCT

(10) International Publication Number
WO 02/49309 A2

(51) International Patent Classification⁷: H04L 29/00

(21) International Application Number: PCT/EP01/14441

(22) International Filing Date: 10 December 2001 (10.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
VI2000A000274 12 December 2000 (12.12.2000) IT

(71) Applicants and
(72) Inventors: **RENIER, Frederico** [IT/IT]; Via Piave 39, I-30171 Mestre (IT). **VIRGILI, Pierluigi** [IT/IT]; Via s. Dona' 160, 30174 Mestre (IT).

(74) Agent: **BONINI, Ercole**; Studio Ing. E. Bonini SRL, Corso Fogazzaro, 8, I-36100 Vicenza (IT).

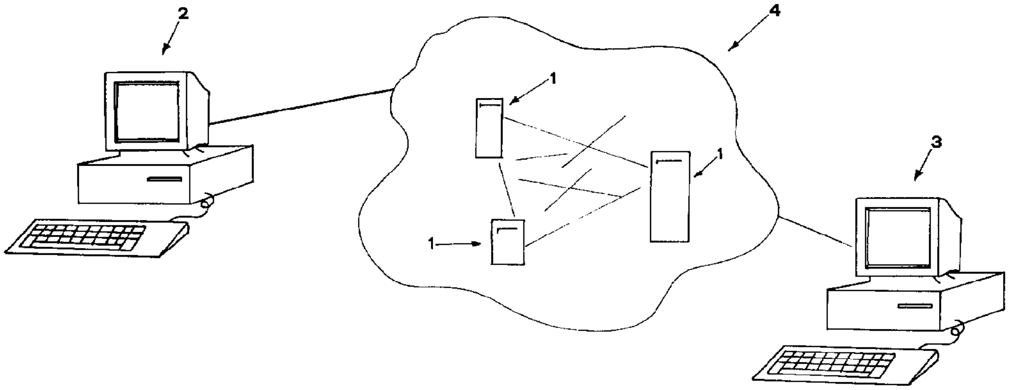
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF CERTIFYING TRANSMISSION, RECEPTION AND AUTHENTICITY OF ELECTRONIC DOCUMENTS AND RELATED NETWORK UNIT



(57) Abstract: A method of certifying transmission, reception and authenticity of electronic documents between a sender user (2) and addressee user (3) belonging to a telecommunication network (4) is disclosed, wherein the sender (2) carries out the following steps: drafting the document to be sent putting the electronic address of addressee (3), sending to a mailbox belonging to the telecommunication network associated to the addressee (3) a message comprising the drafted documents and wherein the addressee (3) carries out the step of downloading the message from the mailbox associated to him. The method provides for the automatic generation of a certificate of transmittal of the message that is being automatically sent to the mailbox of the sender (2) by a certification entity connected to the network when the message reaches the mailbox of the addressee (3).

WO 02/49309 A2

METHOD OF CERTIFYING TRANSMISSION, RECEPTION AND AUTHENTICITY OF ELECTRONIC DOCUMENTS AND RELATED NETWORK UNIT

The present invention relates to a method of certifying transmission, reception and authenticity of electronic documents to be useD as an alternative to postal services delivering normal letters, printed matter, registered letters, insured letters and to electronic mail as well as a network unit adapted to carry out such a method.

It is well known that the development of information systems led the companies to develop internal telecommunications networks called INTRANET, consisting of a plurality of interconnected computers capable of communicating with each other.

In the sixties a global network was also developed called INTERNET that can be defined as a telecommunication network of telecommunication networks and having its extension as main feature.

More particularly the internet network is developed on the whole earth surface and allows anybody having a computer to connect with the network and use the services offered.

More particularly one of the services offered by internet is the electronic mail allowing to send and receive messages, electronic documents, images and anything else to anybody being a member of the network.

More particularly the system provides that both sender and addressee of the electronic message as members of the network, are each provided with at least an e-mail address and a computer having the means required for sending and receiving electronic documents through the net.

It is known that the sender prepares the electronic document containing the information to be sent, and sends it to the addressee giving to the message his address.

The sent message travels on the intranet or internet network passing from one server to the other until it reaches the server having the mailbox associated to the addressee.

The message contained in the mailbox reaches the addressee as soon as the latter connects to the net to check its contents. In this way indeed the addressee starts the procedure of transferring the electronic document to his computer so as to allow its reading.

A first drawback of the described electronic mail system consists in that it doesn't guarantee identity of the sender.

More particularly the system is not able to warrant that the message drafter is actually the person identified by the sender's electronic mail address.

A further drawback linked to the preceding one, consists in that the electronic documents sent and received with such a system do not have a legal validity. This makes necessary using the system of paper mail when a legal validity of the document is required.

In order to overcome said drawbacks the prior art provides for use of the digital signature being the computerized equivalent of the handwritten signature set on the paper documents.

Such a signature is supported by special rules stating that anybody intends to draft and sign computerized documents with legal validity, must obtain the above mentioned digital signature.

More particularly this signature has the same legal validity and identifies in an univocal way, the person who set his signature warranting also that the document received was not altered after signature.

More particularly the digital signature is based on the symmetric cryptography and provides for use of a couple of keys, a private key secretly kept by the holder, and a public key necessary for the addressee to verify authenticity of the signature set by the sender.

As it is known, the two keys consist of a set of only apparently random characters and are interrelated in an univocal way so as to make impossible to go back from the public key to the private key.

The univocal association between public key and the holder of the corresponding private key is warranted by proper certification entities authorized to release and keep said keys.

It is known that the cryptography algorithm is based on the Hash algorithm extracting from the document an imprint constituting a univocal synthesis from which it is not possible to go back to the original document and to which a codification algorithm is subsequently applied using the private key of the user.

This method allows to decode the document to be sent in order to warrant that said document is being read only and exclusively by the intended addressee.

A first drawback of the above described system consists in that it allows to warrant integrity of the sent message and sender's identity but does not warrant the sender that transmittal and delivery of the message to the addressee occurred.

Another drawback consists in that the sender does not know the date and time of the delivery nor the date of opening the document transmitted by him.

The object of the present invention is to overcome the foregoing drawbacks.

More particularly a first object of the invention is to provide a method certifying that the message was sent to the addressee.

Another object of the invention is to provide a method certifying that the addressee read the electronic document sent by the sender.

Another object of the invention is to provide a method allowing transmittal and reception of documents having a legal validity and provided with a transmittal and reception fixed date.

A further object is to propose a method warranting delivery speed and flexibility of the electronic mail system combined with the legal validity of the documents so transmitted.

A last but not least object is to provide a network unit to be connected in said net to carry out the method of the present invention.

The foregoing objects are attained by a method for certifying transmission, reception and authenticity of electronic documents between at least a sender user and at least an addressee user belonging to a telecommunication network wherein according to the main claim, said sender user carries out the following steps:

- drafting the document to be sent setting the electronic address of said addressee user;
- encrypting said document to be sent;
- codifying said encrypted document through a private key;
- sending to a mailbox belonging to said telecommunication network associated with said addressee user, a message comprising said drafted document, said encrypted and codified document and a public key for decoding said codified and encrypted document;

and wherein said addressee user carries out the following steps:

- downloading said message from said mailbox assigned to him;
- decoding said encrypted and codified document through said public key;
- encrypting said document drafted by said sender;
- comparing said encrypted document with said decoded document to verify

authenticity of said received document;

said method being characterized by providing the automatic generation of a message transmittal certificate which is automatically sent to the mailbox of said sender user from a certification entity connected to the net, when said message reaches said mailbox of said addressee.

Advantageously the proposed method allows to check the quantity of information transmitted by the sender in order to charge him the cost of the transmission.

Still advantageously the proposed method allows to charge in an automatic and periodical way the costs relating to the transmissions effected by each sender.

The foregoing method is carried out through a network unit operating as certification entity comprising:

- connection means to said telecommunication network;
- message reception and transmission means from and to said telecommunication network;
- at least a first file unit containing the data of said users and at least an identification code for each of said users;
- processing means for the messages received as input from said transmission and reception means identifying the sender of said messages and checking if said sender is included among the users existing in said at least one file unit so as to admit or refuse said messages;
- at least a second file unit containing the admitted messages; and
- certification means adapted to create certification documents of the transmittal and /or reception of said messages to one or more addressees.

The foregoing objects and advantages will be better understood by reading the following description of a preferred embodiment with reference to the accompanying sheets of drawings in which:

- Fig. 1 is the basic scheme of the telecommunication network to which each sender and addressee are connected;
- Fig. 2 is a block diagram showing the method of the present invention;
- Fig. 3 is a block diagram of the network unit of the invention adapted to carry out the method shown in Fig. 2; and
- Fig. 4 is a block diagram of some elements belonging to the computer of each user provider of the mail service of the invention.

The method of certifying transmission, reception and authenticity of electronic documents between a sender user 2 and an addressee user 3 belonging to a telecommunication network 4 of the present invention provides that as shown in Figs. 1 and 2, the sender user 2 drafts the document to be sent putting the electronic address of the addressee user and encrypts the document with subsequent codification through a private key in his possession. Finally he sends to the mailbox associated to the addressee 3 and belonging to the telecommunication network 4, a message comprising the drafted document, the encrypted and codified document and a public key allowing the decodification of the codified and encrypted document.

The addressee user in his turn downloads the message from the mailbox, decodes the encrypted and codified document through the public key and encrypts the document drafted by the sender.

Finally he compares the encrypted document with the decoded document to check authenticity of the received document.

The invention provides for the automatic generation of a message transmittal certificate which is being automatically sent to the mailbox associated with the sender, also belonging to the telecommunication network, when the message reaches the addressee mailbox.

More particularly said certificate is generated and sent by a certification entity intended for this service and connected to the net.

The invention provides that when the addressee gains access to his mailbox to check its contents and download any message, a certificate of occurred delivery of the message is automatically generated and automatically sent to the mailbox of the sender.

Still according to the invention the addressee when opening the message may send to the sender in a manual or automatic way, a certificate of having read the document sent by the sender informing the latter that the message was actually read.

The method of the invention provides also that at each message exchanged between the user a weight is assigned being a function of the size and type of message, by which cost of transmission to be charged to the sender and or the addressee is calculated.

The method of the invention is carried out as shown in Fig. 1, by connecting to the telecommunication network 2 one or more network units 1 with the function of certification entity provided as shown in the block diagram of Fig. 3, with connection means 5 to said network 4, cooperating with message transmission and reception means 6 to send or receive the messages in the network 2 and mailboxes associated to the users.

More particularly the network unit 1 comprises:

- identification means 7 of the message sender adapted to admit or refuse the messages received by the network;
- identification means 8 of the kind of requested service;
- certification means 9 adapted to generate documents certifying transmittal and /or reception of messages exchanged by user 2, 3 cooperating with means 10 adapted to supply the fixed time and date of reception or transmission of the message or the generated certificate;
- computation means 11 of the message transmittal cost comprising means 12 for measuring size of the messages, cooperating with identification means 13 of the requested service and automatic charging means 14 to the users;
- means 15 generating a copy of the message sent by the sender and of the generated certificates;
- a first non erasable file unit 16 containing for each user of the service a personal identification code and any personal data;
- a second non erasable file unit 17 containing the messages admitted by the corresponding means;
- a third non erasable file unit 18 containing the certificates generated by the corresponding means;
- and a fourth file unit containing the invoices.

The network unit 1 may also comprise encryption and decryption means for the messages sent or received by the network necessary to warrant privacy of transmittal, of a type known per se and therefore not described hereinafter.

As to the users of the service, they are connected to the telecommunication network as diagrammatically shown in Figs. 1 and 4 through a computer.

More particularly the computer comprises:

- connection means 20 to the network 4;
- message transmission and reception means 21;
- encryption and decryption means 22 and codification and decodification means 22;

- means 23 for generating and reading documents and messages;
- a file 24 of received and sent messages;
- means 25 for filing and reading certificates;
- means 26 for filing and reading invoices;
- an addressee file 27.

With regard to the certification document of the document transmittal and the certificate of delivery according to the invention, each of them comprises the identification code of the network unit that received the message and sent the certification document, a declaration of certification of sender's or addressee's identity and the date of reception by the server of the document sent by the sender.

As to the document certifying reading of the message, it comprises the identification code of the addressee who read the message accompanied by a declaration certifying that reading occurred as well as the date of said reading by the addressee.

As to the steps of codification or decodification and encryption and decryption of the documents that could even not be used, they are preferably based on methods of asymmetric cryptography.

As above mentioned said methods provide for using a private key and a public key supplied by a certification entity of the identity of the holder of said keys, identifying univocally the user holder.

The sender user who wants operatively to send a message, uses the document reading and writing means 23 with which his computer is provided and proceeds to encrypt and codify the document following the previously described method, putting the electronic address of the addressee taken from the addressee file 27.

Then he sends to the net the message that is collected by the reception means 6 belonging to the network unit 1 having the mailbox associated with the addressee 3.

The identification means 7 then provide to identify the sender and check that he belongs to the file unit 16 of the service users.

If the sender is not found in the file 16, the message is refused, otherwise it goes to the identification means 8 of the requested service detecting the type of requested service and deciding the subsequent steps to be carried out.

More particularly the identification means 8 recognize whether it is a check of the contents of a mailbox or it is a transmission of a message that must occur with a receipt proving transmittal or delivery or reading occurred.

In the case in question it is a transmission request and therefore the means 9 generating certificates are activated.

These means 9 generate the requested certificate requesting date and time of receipt of the message to the corresponding means 10 and file both the received message and the generated certificate.

At the same time the billing means 11 are activated that charge the cost to the sender 2 according to the size and type of requested service on the base of a schedule of costs contained in a cost file unit 30. More particularly the invoice is filed in a corresponding file unit 31 and possibly sent at the same time to the sender 2.

The certificate so generated is then sent through the transmission means 6 to the mailbox of sender 2 who may or may not belong to the network unit 1 generating said certificate, while the message is deposited in the mailbox of the addressee 3 consisting of the cell of the file 17 of documents to be delivered.

The sender 2 connecting to the net and checking his mailbox may then download a copy of the transmittal certificate that will be filed in the corresponding file 25 with which his computer is provided. Such a certificate gives him the warrant under responsibility of the entity carrier of the network unit 1, that the transmittal of the message to addressee 3 occurred, thus attaining the intended objects.

The addressee 3 intending to download the mail contained in his mailbox, sends such a request to the network unit 1 that once identified both the user and type of requested service, proceeds to activation of the means 15 generating copy of the messages to be delivered downloaded on the computer of addressee 3 as well as activation of the certificate generating means.

These means 15 activate the certification means 9 generating a certificate of delivery to addressee 3 of the message sent by sender 2 in a similar way to the preceding one.

Such a certificate is then sent to the mailbox associated to sender 2 that can therefore download it receiving the warrant under the responsibility of the entity carrier of the network unit 1, that the message was duly delivered to addressees so as to reach the intended objects.

It is important to note that the carrier of the network unit 1 is warranter of all the operations of delivery and custody of the messages that as above stated, are contained in a non erasable file unit.

Such a system thus allows to give legal validity and certitude of occurred transmittal and delivery also to the messages sent using a telecommunication mail system.

According to a non illustrated executive version, the network unit 1 may comprise means for sending SMS messages to a cellular phone belonging to the addressee, said messages being automatically activated to advice him of arrival of a new message or the status of his mailbox.

Alternatively the network unit 1 may supply such a service through means for sending voice messages that could then reach not only mobile telephone sets but also fixed telephone sets.

All the means constituting the network unit may be indifferently formed by microprocessor units, electronic devices of any kind or the operative system of a computer.

Moreover all the filing units may consist of backing storage units such as hard disks or CDROM unit or magnetic support in general.

Moreover the certification entity of the identity of user, sender and addressee, supplying the public and private keys and the certification entity of transmittal and delivery may indifferently consist of a single entity or several different entities.

In the implementing phase, many modifications could be made to the method and to the network unit, that when falling within the scope of the appended claims should be considered covered by the present patent.

CLAIMS

1) A method of certifying transmission, reception and authenticity of electronic documents between at least a sender user (2) and at least an addressee user (3) belonging to a telecommunication network (4) wherein said sender user (2) carries out the following steps:

- drafting the document to be sent putting the electronic address of said addressee user (3);
- sending to a mailbox belonging to said telecommunication network (4) associated to said addressee user (3) a message comprising said drafted document;

and wherein said addressee user (3) carries out the following steps:

- downloading said message from said mailbox associated with him,

characterized by providing the automatic generation of a transmittal certificate of said message that is automatically sent to the mail box of said sender user (2) by a certification entity connected to the net, when said message reaches said mailbox of said addressee (3).

2) The method according to claim 1) **characterized by** providing the automatic generation of a delivery certificate that is automatically sent to the mailbox of said sender user (2) when said addressee (3) gains access to the mailbox associated to him.

3) The method according to any of the preceding claims **characterized by** comprising the following steps:

- checking size of said document;
- calculating cost of said transmittal;
- and billing said cost to said sender (2) and/or said addressee (3).

4) The method according to any of the preceding claims **characterized by** providing the manual and/or automatic transmission by said addressee user (3) to said sender (2) of a certificate of having read said message when said addressee (3) opens said message.

5) The method according to any of the preceding claims **characterized in that** said sender user after the step of drafting said document and before sending said message carries out the following steps:

- encrypting said document to be sent;
- codifying said encrypted document through a private key;

said message comprising also said encrypted and codified document and a public key for decodification of said codified and encrypted document; and in that said addressee user after the step of downloading said message carries out the following steps:

- decoding said encrypted and codified document through said public key;
- encrypting said document drafted by said sender;
- comparing said encrypted document with said decoded document to check authenticity of said received document.

6) The method according to claim 5) **characterized in that** said private key and said public key are supplied by a certification entity of the identity of said users (2, 3), said keys identifying univocally said users (2, 3).

7) The method according to claim 5) or 6) **characterized in that** said codification and decodification and encryption and decryption operations of said documents are based on methods of asymmetrical cryptography.

8) A network unit (1) operating as certification entity adapted to carry out the method according to any of the preceding claims **characterized by** comprising:

- connection means (5) to said telecommunication network (4);
- reception and transmission means (6) of said messages from and to said telecommunication network (4);
- at least a first file unit (16) containing the data of said users (2, 3) including for each user at least an identification code for each of said users (2, 3);
- identification means (7) of the sender of messages received as input from said transmission and reception means (6) identifying the sender (2) of said messages and checking if said sender (2) is included among the users (2, 3) existing in said at least one file unit (16) so as to admit or refuse said messages;
- at least a second file unit (17) containing the admitted messages;
- certification means (9) adapted to generate certification documents of transmittal and/or reception of said messages to one or more addressee (3).

9) The unit (1) according to claim 8) **characterized by** being provided with at least one of said electronic mailboxes associated to said users (2, 3).

10) The unit (1) according to claim 8) or 9) **characterized by** comprising means (11) calculating cost of transmittal of said message to be charged to said sender (2) and/or addressee (3).

11) The unit according to any of claims 8) to 10) **characterized by** being provided with automatic billing means (14) to said sender (2) and/or said addressee (3) of the cost of transmitting said message.

12) The unit according to any of claims 8) to 11) **characterized by** comprising means (10) adapted to supply upon request of said certification means (8), the fixed time and date of reception of said message or transmission of said certificates.

13) The unit (1) according to any of claims 8) to 11) **characterized by** comprising at least a third file unit (18) of said certificates.

14) The unit (1) according to any of claims 8) to 13) **characterized in that** said at least a first file unit (16) of the sent documents is non erasable.

15) The unit (1) according to claim 13) **characterized in that** said at least a third file unit (18) of said certificates is non erasable.

16) The unit (1) according to any of claims 8) to 15) **characterized by** comprising means (15) generating copy of the message sent by said sender (2).

17) The unit (1) according to any of claims 10) or 11) **characterized in that** said means (11) calculating the cost of transmittal of said message comprise means (12) for measuring size of said message cooperating with means (13) identifying the requested service and at least a fourth file unit (31) containing the invoices.

18) The unit (1) according to any of claims 8) to 17) **characterized by** being provided with means for sending SMS messages to a cellular phone of said addressee (3) which are automatically activated to advice said addressee (3) of the status of his electronic mailbox.

19) The unit (1) according to any of claims 8) to 18) **characterized by** being provided with means for sending voice messages to a telephone set of said addressee user (3) that are automatically activated to advice said addressee user (3) of the contents of his electronic mailbox.

20) A computer adapted to carry out the method according to any of claims 1) to 7) **characterized by** comprising connection means (20) to the network (4) cooperating with transmission and reception means (21) of said messages.

21) The computer according to claim 20) **characterized by** comprising encryption and decryption and codification and decodification means (22) of

the messages sent or received by said transmission and reception means (21).

22) The computer according to claim 20) or 21) **characterized by** comprising means (25) for handling and filing said certificates received by said network unit (1).

23) A certification document of transmittal of a correspondence according to any of the preceding claims **characterized by** comprising:

- at least an identification code of the network unit receiving said messages and sending said certification document;
- at least a certification declaration of the sender and the addressee;
- the fixed date of reception of said document sent by said network unit.

24) A certification document of reception of a correspondence according to any of claims 2) to 23) **characterized by** comprising:

- at least an identification code of the network unit receiving said message and sending said certification document;
- at least a certification declaration of the sender and the addressee;
- the fixed date of downloading said document sent by said network unit.

25) A certification document of reading a correspondence according to any of claims 5) to 22) **characterized by** comprising:

- at least an identification code of said addressee having read said message;
- at least a certification declaration that reading of said document occurred by said addressee and
- the fixed date of reading said document sent to said addressee.

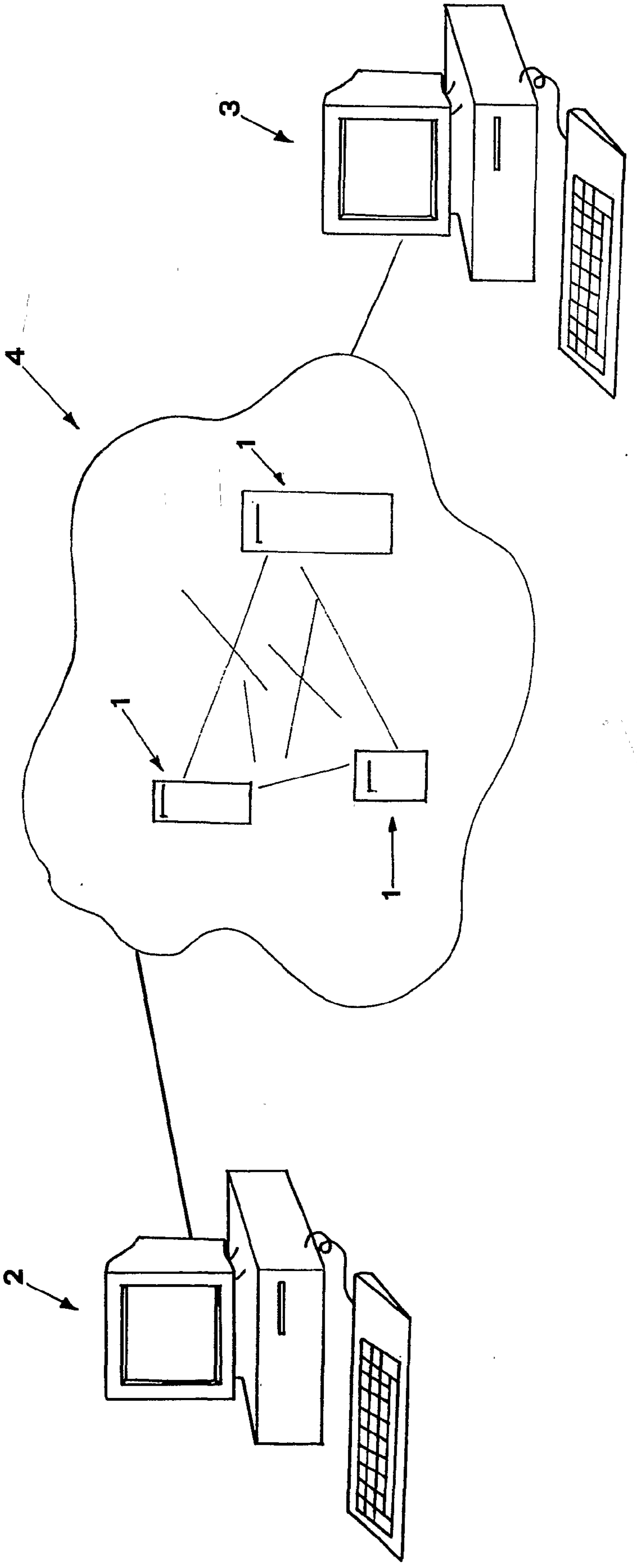


FIG.1

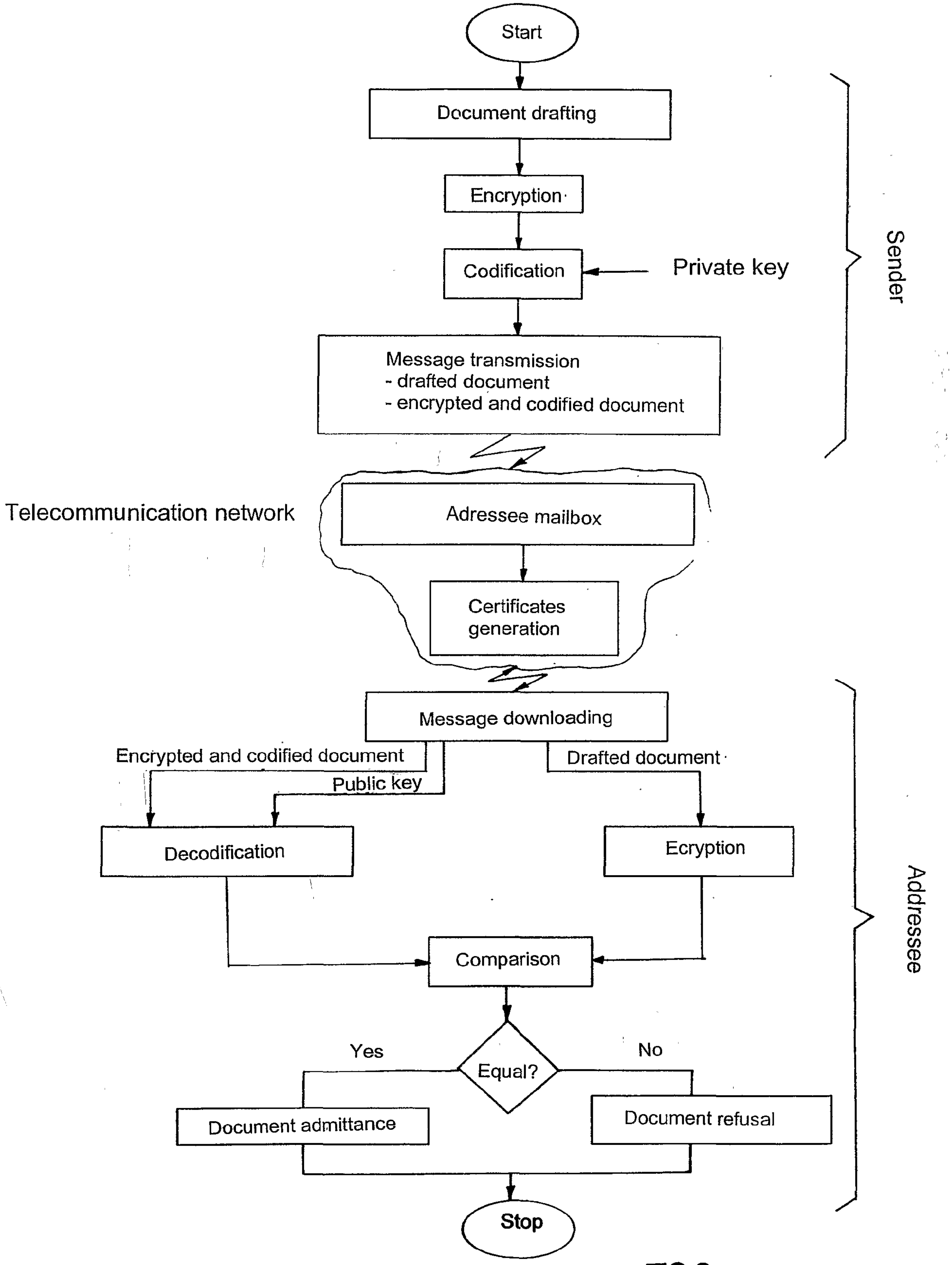

Start
Document drafting
Encryption
Codification
Private key
Sender
Message transmission
- drafted document
- encrypted and codified document
Telecommunication network
Adressee mailbox
Certificates generation
Message downloading
Encrypted and codified document
Public key
Drafted document
Decodification
Ecryption
Addressee
Comparison
Yes
Equal?
No
Document admittance
Document refusal
Stop

FIG.2

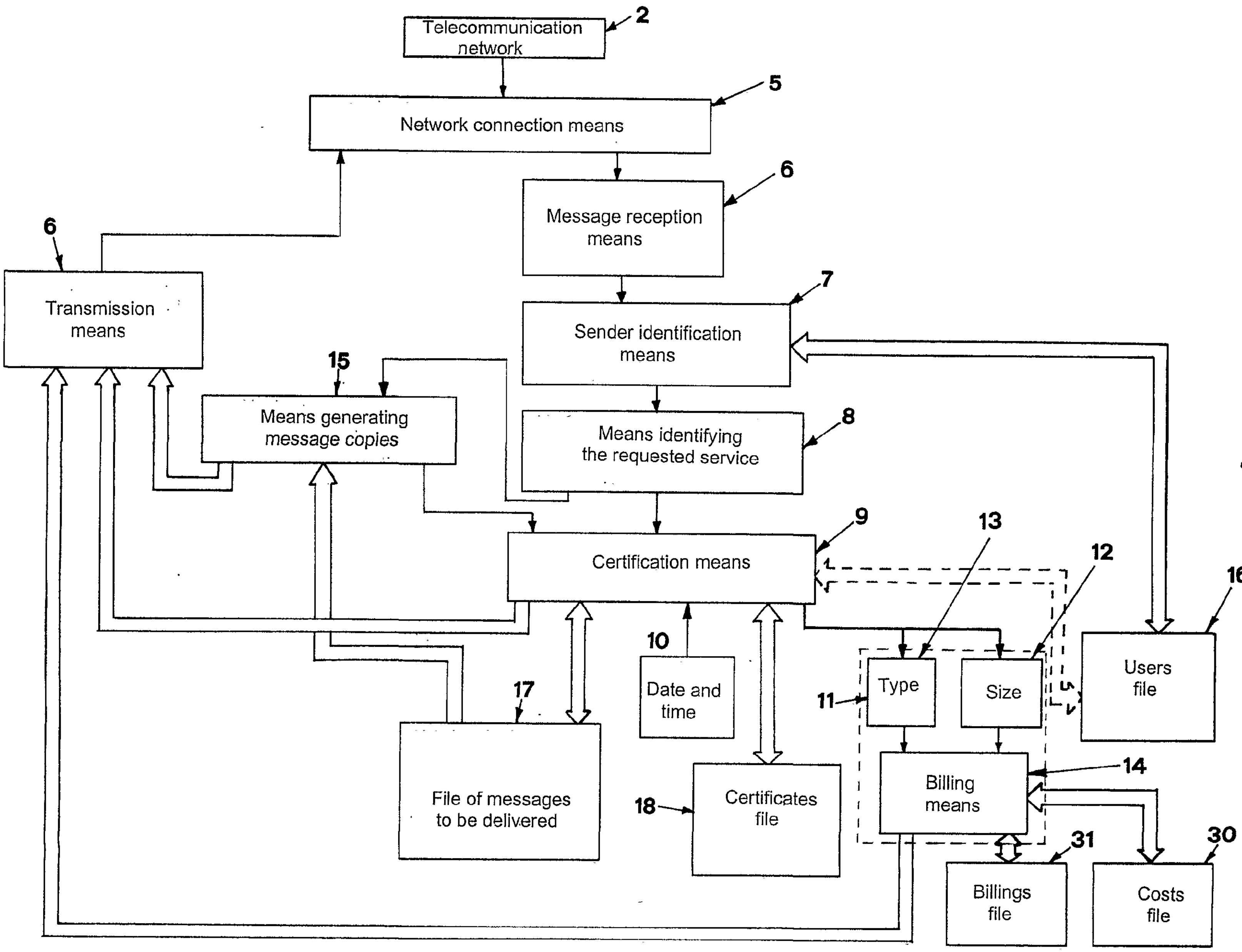

Telecommunication network
2
Network connection means
5
Message reception means
6
Sender identification means
7
Means identifying the requested service
8
Certification means
9
Date and time
10
11
Type
13
Size
12
Billing means
14
Users file
16
Costs file
30
Billings file
31
Certificates file
18
File of messages to be delivered
17
Means generating message copies
15
Transmission means
6

FIG.3

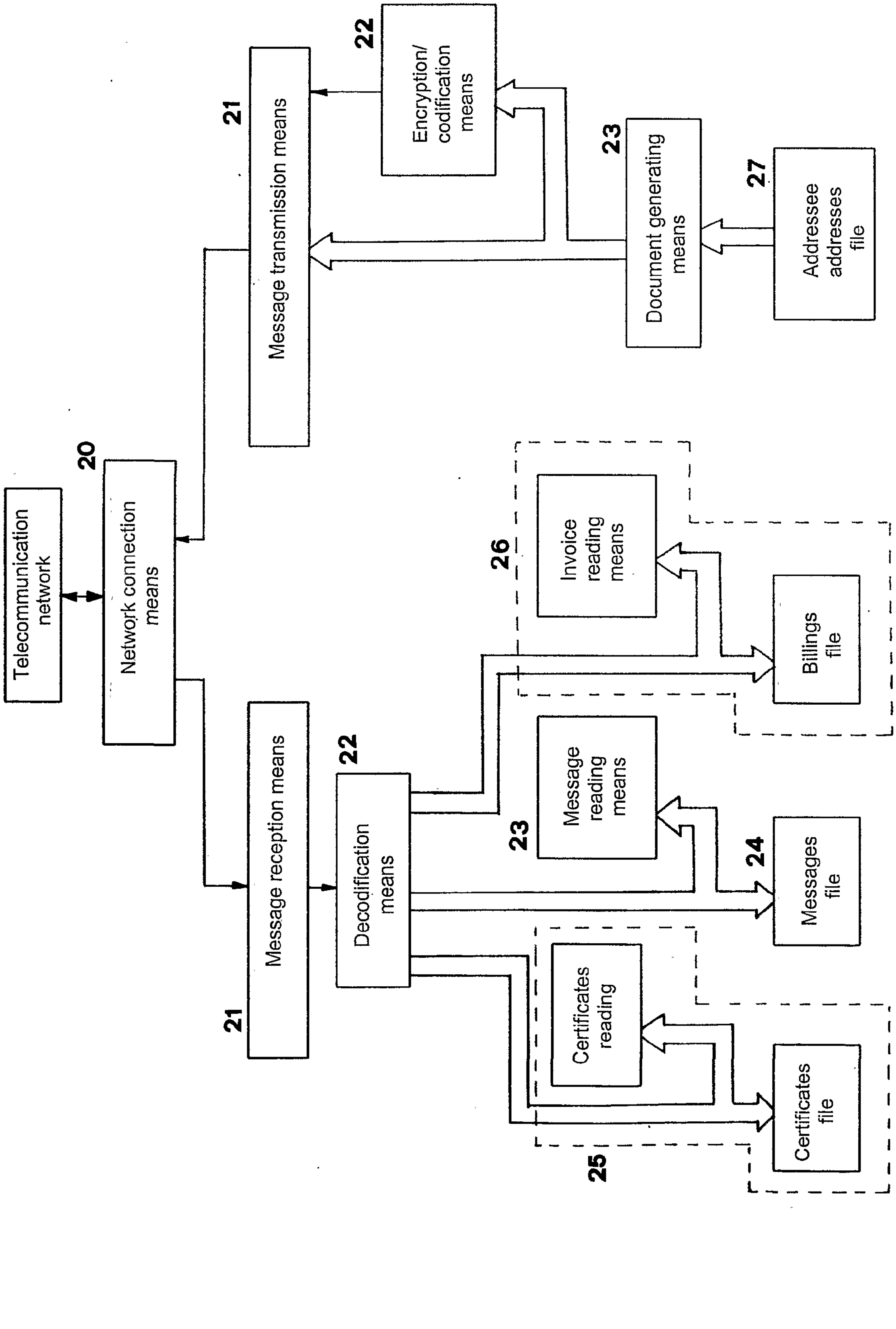

Telecommunication network
Network connection means
20
Message transmission means
21
Encryption/ codification means
22
Document generating means
23
Addressee addresses file
27
Message reception means
21
Decodification means
22
Invoice reading means
26
Billings file
Message reading means
23
Messages file
24
Certificates reading
Certificates file
25

FIG.4